BELLSOUTH

Ben G. Almond
Executive Director-
Federal Regulatory

DOCKET FILE COPY ORIGINAL

Suite 900
1133-21st Street, N.W.
Washington, D.C. 20036
202 463-4112
Fax 202 463-4198

December 18, 1997

RECEIVED
DEC 18 1997
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Ms. Magalie R. Salas
Secretary
Federal Communications Commission
1919 M Street, NW, Room 222
Washington, DC 20554

RE: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information

Dear Ms. Salas:

This is to inform you that on December 18, 1997, A. Kirven Gilbert III, Cynthia T. Ford and Ben Almond, all of BellSouth Corporation met with Ruth Milkman, Blaise Scinto and Dorothy Attwood, all of the Common Carrier Bureau concerning issues associated with the above referenced proceeding.

The focus of the meeting was BellSouth's consistent position that a notification and Opt-Out Process is central to joint-marketing and providing customers the services they expect and need. The discussion centered on one report issued by the Federal Trade Commission (FTC) associated with balancing the privacy protection expectations of the public against the acknowledgement that "individual reference information" is of extreme value to law enforcement agencies, businesses and the general public. The reports highlighted the use of an Opt-Out process to permit consumers access to their own non-public information and restrict distribution of this information to the general public.

In many aspects, this report addressed similar issues raised in the FCC's CPNI proceeding and expressed recognition of the value of an Opt-Out vs. Opt-In process for the information industry to comply with governmental regulations. Attached are copies of the two FTC's reports discussed in the meeting.

Cy 1

Please associate this notification and the accompanying documents with the docket proceeding.

If you have any questions concerning this matter, please contact the undersigned.

Sincerely,

Ben G. Almond

Ben G. Almond
Executive Director-Federal Regulatory

Attachments

Cc: Ruth Milkman
Blaise Scinto
Dorothy Attwood

FOR RELEASE: DECEMBER 15, 1997

FTC SURFS CHILDREN'S WEB SITES TO REVIEW PRIVACY PRACTICES: Most Are Collecting Data on Kids; Few Seek Parental Approval

Federal Trade Commission staff announced today the results of "Kids Privacy Surf Day" designed as a "snapshot" of children's Web sites' privacy practices. FTC staff found that approximately 86 percent of the sites surveyed were collecting personally identifiable information from children -- most without seeking parental permission or allowing parents to control the collection and use of the information. FTC staff surveyed 126 Web sites listed by "Yahooligans!," a popular directory of child-oriented sites.

The Mini-Surf was not intended to be a comprehensive survey, but a quick "snapshot" to see what child-oriented Web sites are doing to inform parents about their information gathering practices. Approximately 86 percent of the sites surveyed were collecting personally identifiable information from children -- names, e-mail addresses, postal addresses and telephone numbers. Fewer than 30 percent of those sites collecting this personal data posted either a privacy policy or a confidentiality statement on their Web site. Four percent of those sites collecting personally identifiable information required parental authorization for the collection of the information.

"Protecting children's privacy online is a high priority," said Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection Bernstein. "Any company that engages in deceptive or unfair practices involving children violates the FTC Act. The FTC can bring legal action to halt such violations and seek an order imposing restrictions on future practices to ensure compliance with the FTC Act.

"Industry has proposed self-regulatory guidelines to govern the collection and use of children's information, and we know that industry trade associations are working hard to promote these self regulatory guidelines to their members," Bernstein added. "This survey 'snapshot' demonstrates that these guidelines need to be more broadly implemented. FTC staff will be conducting a systematic review of Web sites' information collection practices in March 1998 to report to Congress on the extent to which Web sites, including children's Web sites, are posting privacy policies."

The FTC staff last July issued an opinion letter to the Center for Media Education, describing certain information collection practices which could be found to be deceptive or unfair. A copy of the staff opinion letter is available at the FTC Web site at ***http://www.ftc.gov/os/9707/cenmed~1.htm*** *(no period)*

FTC staff will send the Web sites surveyed in the Mini-Surf e-mail messages notifying them about the FTC staff opinion letter and the principles it contains. The messages note that according to FTC staff, (1) it is a *deceptive practice* expressly or impliedly to misrepresent the purpose for which personally identifiable information is being collected from children, and (2) it is likely to be an *unfair practice* to collect personally identifiable information from children and sell or otherwise disclose that information to third parties without providing parents with adequate notice and an opportunity to control the collection and use of the information. The e-mail also states that FTC staff has not determined that the online information collection practices of the site have violated federal law.

The Kids Privacy Surf Day was conducted October 14, 1997.

Consumer education materials and information addressing online privacy issues are available on the Internet at the FTC's World Wide Web site at *http://www.ftc.gov* and also from the FTC's Consumer Response Center, Room 130, 6th Street and Pennsylvania Avenue, N.W., Washington, D.C. 20580; 202-326-3128; TTY for the hearing impaired 202-326-2502. To find out the latest news as it is announced, call the FTC NewsPhone recording at 202-326-2710.

# # #

MEDIA CONTACT:
Claudia Bourne Farrell
Victoria Streitfeld
Office of Public Affairs
202-326-2181 or 202-326-2180

STAFF CONTACT:
Toby M. Levin
Bureau of Consumer Protection
202-326-3156

(kids)

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Bureau of Consumer Protection

July 15, 1997

Kathryn C. Montgomery, President
Jeffrey A. Chester, Executive Director
Center for Media Education
1511 K Street, NW
Suite 518
Washington, D.C. 20005

Re: Petition Requesting Investigation of, and Enforcement Action Against SpectraCom, Inc.

Dear Ms. Montgomery and Mr. Chester:

On May 13, 1996, the Center for Media Education (CME) filed a petition requesting that the Commission investigate and bring a law enforcement action for alleged deceptive practices in the operation of an Internet Web site called "KidsCom," then operated by SpectraCom, Inc.(1) The site is now operated by an affiliated entity, The KidsCom Company (hereinafter, both are referred to as KidsCom). Our review of this matter indicates that certain of KidsCom's practices likely violated Section 5 of the Federal Trade Commission Act. For several reasons, including the fact that KidsCom has modified its conduct, we have decided not to recommend enforcement action at this time. To provide guidance in this area, however, we are providing our analysis of the practices involved in this Web site, and are setting forth several broad principles we believe apply generally to online information collection from children.

BACKGROUND

KidsCom is a Web site that describes itself as "[a] Communications Playground for kids ages 4 to 15." Children with a computer, a modem, and a Web browser can access KidsCom through the Internet.(2)

At the time of your petition, when children first accessed the KidsCom site, they were required to register by completing the "Who Do You Wanna Be?" survey, which requested them to answer a number of questions about themselves, including their name, sex, birthday, e-mail address, home address, number of family members, and grade.(3) They then had access to the rest of the site, which consisted of a number of connected activity sections including, among others, "Find A Key Pal," which matched children for e-mail "pen pal" correspondence; the "Graffiti Wall," a chat room for children; "KidsKash Questions," which provided an opportunity to earn KidsKash points used to redeem prizes at the "Loot Locker;" and "New Stuff For Kids," which provided information about various new products. In the "KidsKash Questions" portion of the site, children were asked to provide their full name and e-mail address and to answer questions about their product and activity preferences.

This letter addresses two issues raised by CME's petition with regard to KidsCom's practices. First, the petition alleges that the KidsCom site was used to solicit personal information from children in a deceptive manner. It charges that KidsCom failed to fully and accurately disclose the purpose for which it collected the information and the uses

that it made of it. Second, the petition asserts that KidsCom deceptively portrayed KidsCom as independently and objectively endorsing products, when in fact the "endorsements" were essentially disguised advertising.

THE COLLECTION OF PERSONAL INFORMATION

The staff has conducted an investigation of KidsCom's collection and use of children's personal information through the KidsCom Web site,(4) and concluded that certain of KidsCom's information practices may have violated Section 5 of the Federal Trade Commission Act.

Deception

The "KidsKash Questions" area of the Web site awarded "KidsKash" to children who answer surveys containing detailed questions regarding, among other things, their preferences with respect to specific products. These surveys were optional. Information collected from some of these surveys was provided to private companies on an aggregate, anonymous basis.(5)

As you know, Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. 45, prohibits unfair and deceptive practices that are in or affecting commerce. A representation, omission or practice is deceptive if it is likely to mislead reasonable consumers in a material fashion.(6) When KidsCom collected information at the KidsKash Questions area, it represented that the information collection would enable the children to earn premiums, but did not also disclose the marketing uses of this information. It is a deceptive practice to represent that a Web site is collecting personally identifiable information from a child for a particular purpose (*e.g.*, to earn points to redeem a premium), when the information will also be used for another purpose which parents would find material,(7) in the absence of a clear and prominent disclosure to that effect.(8)

Moreover, in order to be effective, any disclosure regarding collection and use of children's personally identifiable information must be made to a parent, given the limited ability of many children within the target audience to comprehend such information. While the KidsCom site, from time to time, did feature notices advising children to seek parental consent before participating in KidsCom or completing surveys, we agree with petitioner that these disclosures were inadequate to notify children or parents that the personally identifiable information solicited was intended for marketing research purposes.

An adequate notice to parents should disclose: who is collecting the personally identifiable information, what information is being collected, its intended use(s), to whom and in what form it will be disclosed to third parties, and the means by which parents may prevent the retention, use or disclosure of the information.(9)

Unfairness

On the KidsCom site, the "Who Do You Wanna Be?" registration survey asked questions about children's preferences and was mandatory for gaining access to most other portions of the site. Some of the information collected at this area of the site was used in the site's Key Pal (online pen pal) program, if the child wanted to participate in that activity. Thus, a child's first name, age, e-mail address and areas of interest were made available to other registrants, in order that they could become "key pals."(10)

A practice is unfair under Section 5 if it causes, or is likely to cause, substantial injury to consumers which is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or competition.(11) We believe that it would likely be an unfair

practice in violation of Section 5 to collect personally identifiable information, such as name, e-mail address, home address or phone number, from children and sell or otherwise disclose such identifiable information to third parties without providing parents with adequate notice, as described above, and an opportunity to control the collection and use of the information. As we learned at the recent Privacy Workshop, the release of children's personally identifiable information to third parties creates a risk of injury or exploitation of the children so identified.(12) The release of children's information through the KidsCom Key Pal program, without providing parents with adequate notice and an opportunity to control the information, raised just such risks. For example, it is possible that an adult posing as a child could have used the Key Pal program to contact a child directly. In such a circumstance, we believe that *before* releasing individually identifiable data about children, the company should obtain parental consent.

PRODUCT ENDORSEMENTS

CME's petition also alleges that the "New Stuff for Kids" section of KidsCom contained deceptive product endorsements. In that section, KidsCom posted information about various products along with the following statement:

> KidsCom kids said that they want to know about new things just for kids... So we will post updates for you here as we get them. And, if you want us to do some investigative snooping on something of interest to you ... [j]ust e-mail us ... and we will do our best to find it out for you.

The petition asserts that KidsCom represented that the information contained in New Stuff for Kids constituted an independent and objective endorsement of the featured products. In fact, according to the petition, KidsCom solicited new product press releases from manufacturers for this section, and required manufacturers to donate products valuing at least $1,000 to obtain the "endorsement." It appears that the donated products may have been used as prizes purchased by children with the KidsKash they earned.

The passing off of an advertisement as an independent review or endorsement is a deceptive practice under Section 5 of the FTC Act. This is based on the common sense notion that independent product evaluations are material to consumers, *i.e.*, that consumers reading what appears to be an independent review or news report about a product are likely to give it more credence than they would give what they know to be an advertisement.(13) KidsCom's practice of portraying the product information in the New Stuff for Kids section as stemming from an independent appraisal, and its failure to clearly and conspicuously disclose in a manner understandable to children that the information was solicited from the manufacturers and printed in exchange for in-kind payment, was likely to mislead reasonable consumers.

CONCLUSIONS

Notwithstanding our belief that the practices identified above likely violated Section 5, we are not recommending that the Commission take enforcement action at this time. This decision is based on several factors.

First, KidsCom has modified its Web site in significant respects. KidsCom now sends an e-mail to parents when children register at the site, providing notice of its collection practices. Parents are provided with the option to object to release of information to third parties on an aggregate, anonymous basis. Most importantly, KidsCom does not release personally identifiable information (in the form of Key Pal information) to third parties without *prior* parental approval. KidsCom currently requires that parents return by facsimile or postal mail a signed authorization. KidsCom also now discloses to the site visitor the purposes for which it is collecting the information. With regard to the deceptive endorsements, KidsCom has eliminated the statement quoted in the previous

section regarding the product evaluations and expressly states (when this is the fact) that the products' descriptions are obtained from the manufacturer. Additionally, KidsCom has introduced The Ad Bug™, a cartoon icon, which together with other textual material is designed to identify the presence of advertising in the New Stuff for Kids section and other site locations.

Second, there is no evidence that KidsCom at any time released any personally identifiable information to third parties for commercial marketing or any other purposes (other than for the Key Pal program). Such practices would have been of particular concern in light of the absence of adequate disclosure and prior parental consent.

Third, the collection of information from children on the Internet is widespread.(14) Thus, the legal principles implicated here have broader application to other marketers. In light of the rapidly growing technological development and commercial expansion on the Internet, we believe that it is appropriate to issue this letter to provide notice of our interpretation of the relevant legal standard.

In light of the foregoing, the staff has determined not to recommend that the Commission initiate a law enforcement action against KidsCom at this time. We will continue to monitor KidsCom, as well as other commercial Web site operators, to ascertain whether they may be engaged in deceptive or unfair practices. Hereafter, staff may recommend law enforcement proceedings against marketers who engage in deceptive information practices, or who unfairly use personally identifiable information collected from children.

We encourage your continued participation in developing the issues and solutions to protecting privacy online. Petitions from groups such as yours are a helpful means of reviewing possible unfair or deceptive practices, and we hope you will continue to bring to our attention any advertising or marketing campaign that you believe may violate the FTC Act.

Sincerely,

Jodie Bernstein,
Director

(1)CME has submitted several reports and letters to the Commission on this and related subjects. On March 28, 1996, CME submitted its report, "The Web of Deception," outlining concerns regarding online practices targeted to children and asking for an investigation of site practices and implementation of certain principles. On June 5, 1996, in conjunction with the Consumer Federation of America, CME submitted proposed guidelines for online practices. This submission was supplemented on June 19, 1996. On November 25, 1996, and again on June 12, 1997, CME provided additional examples of online collection practices that it considers to be unfair or deceptive.

This letter is responsive to CME's submissions insofar as they raised concerns regarding information collection and endorsement practices at the KidsCom site. CME's requests for issuance of principles or guidelines remain under consideration. With regard to CME's request for action against other sites in connection with information collection practices, staff will reevaluate the practices of those sites after the issuance of this letter, in light of the principles set forth herein. CME's request for Commission action to address issues of commercialization on children's sites will be addressed separately.

The views expressed herein are those of the Bureau of Consumer Protection and do not necessarily represent the view of the Commission or any individual Commissioner.

(2)The KidsCom site is located at http://www.kidscom.com.

(3)The "grade" choices include "kindergarten." Petition at 6.

(4)In connection with the Bureau of Consumer Protection's Internet Privacy Initiative, Commission staff also has conducted public workshops evaluating privacy on the Internet. This initiative began with the Bureau's April 1995 public workshop on Consumer Privacy and the Global Information Infrastructure, which explored consumer issues arising from new technologies such as the Internet. In June 1996, the

Bureau held a public workshop specifically designed to evaluate privacy, including children's privacy, on the Internet. *See, Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996. Finally, in June 1997, the Bureau conducted a follow-up workshop on Internet privacy issues, including consideration of the privacy issues posed by the computer databases known as "look-up services;" evaluation of the status of technological and self-regulatory responses designed to address online privacy; and examination of online collection practices as they pertain to children's information, including examination of mechanisms for implementing information principles such as notice and parental consent.

(5)A SpectraCom marketing brochure stated: "When it comes to children's attitudes and opinions, KidsCom can provide answers. If you're introducing a new product or need to gauge reaction to a concept or service, KidsCom offers a fast, efficient way to conduct your research."

(6)Federal Trade Commission Policy Statement on Deception, *appended to, Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984).

(7)For example, survey evidence introduced at the June Privacy Workshop indicates: 64% of parents say it is not acceptable to ask children to provide their e-mail names to gather statistics on how many children visit a site and what they do at the site; 56% say it is not acceptable to ask children to provide their e-mail name along with their interests and activities in order to gather information on product improvement; 72% say it is not acceptable to ask children to provide their real names and addresses when they purchase products or register to use a site and use this information only within that company; and 97% say it is not acceptable to ask children to provide their real names and addresses when they purchase products or register to use a site and rent or sell those names to other companies. "Commerce, Communication and Privacy Online," Louis Harris/Alan F. Westin Survey, *Privacy & American Business*, 1997.

(8)See, e.g., Beneficial Corp., 86 F.T.C. 119 (1975), *aff'd in part and rev'd in part on other grounds*, 542 F.2d 611 (3d Cir. 1976), *cert. denied*, 430 U.S. 983 (1977) (deceptive to fail to disclose to consumers that information they provided to tax preparer would be used to solicit loans); *Equifax, Inc.*, 96 F.T.C. 844 (1980), *rev'd on other grounds*, 678 F.2d 1047 (11th Cir. 1982) (deceptive to represent, inaccurately, that medical information would be released only to insurance companies); *H&R Block, Inc.*, 80 F.T.C. 304 (1972) (consent), *modified*, 100 F.T.C. 523 (1982) (deceptive for tax preparer to fail to disclose use of tax information for purposes other than tax preparation).

(9)In response to CME's complaint, staff also reviewed whether KidsCom engaged in deceptive or unfair practices in connection with the Graffiti Wall, tracking technologies, or micro targeting. With regard to the Graffiti Wall, it appears that KidsCom discourages children from placing individually identifiable information, such as full names or e-mail addresses, on the Graffiti Wall; clears the log of information placed on the Wall twice each day; does not use the Wall, or information placed on the Wall, for marketing research; and uses information obtained from the Graffiti Wall only as needed to address violations of its rules for participating there (such as swearing).

Tracking technologies, such as click stream data and cookies, permit a site to record the details of a child's site activities. KidsCom does not have or utilize cookies. Additionally, KidsCom does not use click stream technology that permits it to keep a log of the progress of a specific computer as its user progresses through the site. KidsCom becomes aware that a particular child has visited a specific site page only when an already-registered child inputs his or her name to claim KidsKash points for participating in an activity there. This information is not tied to click stream data, not turned over to third parties and is not used for marketing research purposes.

Finally, CME has requested that the Commission evaluate online "micro targeting," which it describes as the development of an advertising pitch specifically tailored to an individual child, based upon information obtained from data collection techniques. Staff's investigation reveals that KidsCom does not engage in such practices.

(10) With this exception, it appears that information collected through the registration form was not released to third parties, in either individually identifiable or aggregate format.

(11)15 U.S.C. 45 (n).

(12)Of particular concern would be uses of information that create the possibility of access by child predators. Department of Justice and Federal Bureau of Investigation representatives speaking at the June 1997 Privacy Workshop (see n. 4) confirmed that publication on the Internet of children's personally identifying information can make them subject to approach by predators. Moreover, it appears that use of computer telecommunications is rapidly becoming one of the most prevalent techniques by which pedophiles identify and recruit children for sexually illicit relationships. *See also Statement of Louis J. Freeh before the Senate Appropriations Committee, Subcommittee on the Departments of Commerce, Justice and State, the Judiciary, and Related Agencies*, April 8, 1997.

(13)See, e.g., Georgetown Publishing House, C-3673 (November 22, 1996) (consent order) (challenging as deceptive an advertisement mailed to consumers that looked like an independent book review that had been ripped out of a publication and mailed to them by an acquaintance); *National Dietary Research, Inc.*, D-9263 (November 7, 1995) (consent order) (alleging deceptive format in advertisements that looked like newspaper articles); *JS&A Group, Inc.*, 111 F.T.C. 522 (1989) (consent order) (challenging format of infomercial that appeared to be independent television show evaluating sunglasses); Commission Advisory Opinion No. 191, 73 F.T.C. 1307 (1968) (stating opinion that a newspaper ad mimicking the format of a restaurant review was deceptive). *See also Nutri/System, Inc.*, 116 F.T.C. 1408 (1993) (consent order) (advertisements cited evaluation and rating of diet programs that appeared in an article in Healthline magazine, implying that the advertiser had no material connection with the publication of the ratings, when in fact the advertiser paid a sponsorship fee to the magazine and received and exercised a right of prior review of the article). Historically, maintaining a clear distinction between advertising and editorial content is even more important when dealing with children than with adults, because children have difficulty distinguishing program content from commercial matter. *See* Broadcast and Cable Services; Children's Television Programming, 56 Fed. Reg. 19611, 19615 (1991).

(14)See Staff Report, Public Workshop on Consumer Privacy on the Global Information Infrastructure, December 1996, Appendix E.

FOR RELEASE: DECEMBER 17, 1997

INFORMATION INDUSTRY VOLUNTARILY AGREES TO STRONGER PROTECTIONS FOR CONSUMERS, FTC SAYS

Social Security Numbers, Birthdates, and Mother's Maiden Names No Longer Available to General Public

In response to growing public and Congressional concern that technology is allowing increased access to sensitive personal information, the Federal Trade Commission today released a report that discusses new industry principles to limit the availability of certain types of personal information. The industry also will allow consumers access to their own non-public information and to opt-out of the non-public information distributed to the general public. In addition, industry has agreed to undergo annual compliance reviews, the results of which will be made public.

The Commission's study analyzed computerized databases -- services that disseminate personal identifiable information, often referred to as "individual reference services" or "look-up services" -- which are used to locate, identify, or verify the identity of individuals. The report summarizes how these services work, examines their risks and benefits, and details the self-regulatory principles that will, among other things, prohibit distribution to the general public of Social Security numbers; mother's maiden names; and dates of birth, if obtained from non-public sources.

"Consumers have been justifiably concerned about the extent to which their personal information has become publicly available," FTC Chairman Robert Pitofsky said in releasing the report to Congress. "The information industry's innovative and far-reaching, self-regulatory program will go a long way to address these concerns and lessen the risk that these services will be misused. The industry should be commended for its responsiveness and commitment.

"Certain important issues regarding consumers' access to public information obtained or compiled by the look-up services remain, however. The Commission is concerned that individuals have no way of discovering or correcting errors that may have occurred in the transcription, transmission, or compilation of this information. We trust the industry will bring the same spirit of cooperation to resolving these remaining issues. We also encourage industries doing business on-line to develop similar self-regulatory efforts to protect consumers' privacy," Pitofsky added.

According to the report, a great deal of information about consumers is available through these individual reference services. This often sensitive personal identifying information comes from a variety of public and non-public sources. Most look-up services operate through their own proprietary networks. Advances in computer technology have allowed consumers' personal identifying information to be aggregated and accessed more easily and cheaply than ever before, often without their knowledge or consent. Surveys show that consumers are increasingly concerned about the use of their personal information. Today, through the use of computers and the Internet, vast amounts of personal information about consumers can be accessed as a result of a simple search. "The present challenge is to protect consumers from threats to their psychological, financial and physical well-being while

preserving the free flow of truthful information and other important benefits of individual reference services," the Report says.

The FTC report, titled "Individual Reference Services: A Report To Congress," was requested by Senators John McCain (R-AZ), Ernest Hollings (D-SC), and Richard Bryan (D-NV) and former Senator Larry Pressler (R-SD).

"I appreciate the work of the FTC and the industry on this important issue. I am particularly pleased with the prospect for a framework of industry self-regulation. I look forward to working with all parties on these important issues," said Senator McCain, Chairman of the Senate Commerce Committee.

"I am encouraged by the progress made by the Federal Trade Commission and the individual reference services industry to address consumer privacy issues involved in 'look-up services.'" said Senator Bryan. "While the efforts at self-regulation by the industry could serve as a model to duplicate elsewhere, we must not give up on our efforts to ensure the standards are adequate to protect against identity theft and other threats to consumer privacy. It is clear that continued oversight is warranted and I will be requesting that the Commerce Committee hold hearings on this issue in the coming year."

Congressman Billy Tauzin (R-LA), Chairman of the House Telecommunications, Trade and Consumer Protection Subcommittee, said, "I am very pleased that industry has stepped up to the plate with serious self-regulation that protects individual privacy while preserving the many beneficial uses of the databases. This is an important first step toward ensuring the privacy of users, while keeping government intrusion at a minimum."

The Report gives an overview of the types and sources of personal identifying information available. It explains that information about a person comes from public sources, such as real property records; marriage and divorce records; birth certificates; driving records; court records; postal records; and government applications, as well as from non-public sources, including survey data and credit and marketing information. Other sources of information about a person also can now be found using the Internet to access published materials, phone numbers and addresses, and information from Web sites where people publish their own identifying information.

"Convenient access to so much information about individuals through individual reference services confers myriad benefits on users of these services and on society. The look-up services enable law enforcement agencies to carry out their missions, public interest groups to find missing children, banks and corporations to prevent fraud, journalists to report the news, lawyers to locate witnesses, and consumers to find lost relatives," the Report states.

At the same time, the Report acknowledges that the increasing availability of this information poses various risks, including a potential threat to individual privacy and harm from unlawful uses of personal identifying information, such as identity theft and credit card fraud.

In addition, "[g]iven the ease with which information can be gathered, aggregated, and shared, errors could be widely replicated and the harm long-lasting."

Last June during the Commission's Workshop on Consumer Privacy, the information industry submitted an initial set of draft self-regulatory principles to protect consumers. The

signatories to the principles include companies that directly offer individual reference services, information vendors, and the three national credit reporting bureaus. As a result of the agreement, the primary sources of non-public and public information have agreed not to sell personal identifying information to those who will not abide by the principles.

According to the Commission's Report, the principles address most concerns raised by the dissemination of non-public personal identifying information. They "impose restrictions on access to . . . 'non-public information' . . . [that will] vary according to the category of customer. . . . In general, customers that have less restricted access to non-public information are subject to greater controls. Conversely, the general public has more restricted access to non-public information . . . "

According to the voluntary industry principles agreed to by the signatories.

- Individual reference services will not distribute to the general public certain non-public information, such as Social Security number, mother's maiden name, birth date, credit history, financial history, medical records, or similar information, or any information about children.

- They also will not make available unlisted telephone numbers obtained from sources other than public records, or unlisted addresses obtained from the telephone company.

- Look-up services may not allow the general public to run searches using a Social Security number as a search term.

- Consumers will be allowed to obtain access to the non-public information maintained about them and to opt-out of the non-public information distributed to the general public.

- Look-up services may not make available information gathered from marketing transactions.

According to the Report, the look-up services must maintain facilities and systems that will prohibit unauthorized access to non-public information. They also must undergo an annual compliance review by a third-party, the results of which will be made public. "This compliance assurance mechanism will curb misuse of non-public, personal identifying information and should significantly affect the practices of the entire individual reference service industry," Pitofsky said.

The Report points out, however, that "[d]espite the laudable efforts . . . important issues related to individual reference services remain." The principles do not provide any limitations "on the availability or uses of public records and publicly available information. Accordingly, they do not limit the potential harm that could stem from access to and exploitation of sensitive information in public records and publicly available information." In addition, they "fail to provide individuals with a means of accessing public records and other publicly available information maintained about them by individual reference services."

The Report concludes with several recommendations that address other concerns left unresolved by the industry proposal. One of the most important of those recommendations "[e]ncourages public agencies to consider the potential consequences associated with the

increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices."

The Commission vote to authorize release of the Report was 4-0.

Copies of the Report, **"Individual Reference Services: A Report To Congress,"** the agenda and transcripts from the FTC's June 1997 Privacy Week, a December 1996 FTC report on consumer privacy, and FTC press releases are available on the Internet at the FTC's World Wide Web site at *http://www.ftc.gov* (no period). FTC documents also are available from the FTC's Consumer Response Center, Room 130, 6th Street and Pennsylvania Avenue, N.W., Washington, D.C. 20580; 202-326-3128; TTY for the hearing impaired 202-326-2502. To find out the latest news as it is announced, call the FTC's NewsPhone recording at 202-326-3710.

MEDIA CONTACT:

Victoria Streitfeld
Office of Public Affairs
202-326-2718

STAFF CONTACT:

David Medine
Bureau of Consumer Protection
202-326-3224

Lisa Rosenthal
Bureau of Consumer Protection
202-326-3224

(FTC File No. P974 806)

(inrefser)

Individual Reference Services

A Report to Congress

Federal Trade Commission

December 1997

Federal Trade Commission

Robert Pitofsky, Chairman
Mary L. Azcuenaga, Commissioner
Roscoe B. Starek, III, Commissioner
Sheila F. Anthony, Commissioner

Executive Summary

In the past year, there has been growing public concern about computerized databases that collect and disseminate personal identifying information about consumers. At the request of three United States Senators, the Federal Trade Commission has conducted a study of computerized database services that are used to locate, identify, or verify the identity of individuals, often referred to as "individual reference services" or "look-up services." The Commission has gathered information about the individual reference services industry by soliciting public comments and holding a public workshop in June 1997. At the workshop, industry members announced that they had formed the "Individual Reference Services Group," or "IRSG Group" and intended to draft a self-regulatory framework to address concerns associated with their industry. Commission staff has worked with this group to encourage it to adopt an effective self-regulatory proposal.

This report summarizes what the Commission has learned about the individual reference services industry, examines the benefits, risks, and potential controls associated with these services, and assesses the viability of the IRSG Group's proposal. The report concludes with recommendations that address concerns left unresolved by the proposal.

A vast amount of information about consumers is available through individual reference services. This information is gleaned from various public sources, such as public records and the telephone directory, and non-public sources, such as "credit header" information from credit bureaus (which typically contains name, aliases, birth date, Social Security number, current and prior addresses, and phone number). Information contained in individual reference services' databases ranges from purely identifying information, *e.g.*, name and phone number, to much more extensive data, *e.g.*, driving records, criminal and civil court records, property records, and licensing records.

Convenient access to so much information about individuals through individual reference services confers myriad benefits on users of these services and on society. The look-up services enable law enforcement agencies to carry out their missions, public interest groups to find missing children, banks and corporations to prevent fraud, journalists to report the news, lawyers to locate witnesses, and consumers to find lost relatives. At the same time, the increasing availability of this information poses various risks of harm to consumers. One harm is to consumers' privacy interests; many consumers are increasingly concerned that personal information is so widely available. Consumers also may be harmed in more concrete ways. For instance, the easy availability of this information could lead to increased incidence of identity theft.

The IRSG Group has developed and agreed to a set of principles that regulates the availability of information obtained from non-public sources through individual reference services by implementing the voluntary restrictions described in this report. Restrictions on access to certain non-public information vary according to the category of customer; customers that have less restricted access to non-public information are subject to greater controls. It is particularly noteworthy that the principles prohibit distribution to the general public of certain non-public information, including Social Security number, mother's maiden name, and date of birth. In addition, consumers will be able to access the non-public

information maintained about them in these services and to prevent the sharing (*i.e.* "opt out") of the non-public information distributed to the general public.

Most importantly, the principles show particular promise because they include a compliance assurance mechanism and are likely to influence virtually the entire individual reference services industry. Members must undergo an annual compliance review by a third-party, the results of which will be made public, and members that are information suppliers are prohibited from selling to entities who fail to comply. Thus, the principles should substantially lessen the risk that information held by these services will be misused, and they should address consumers' concerns about the privacy of non-public information about them in the services' databases.

The Commission commends members of the IRSG Group for the commitment and concern they have shown in drafting and agreeing to comply with an innovative and far-reaching self-regulatory program. The principles address most of the concerns associated with the increased availability of non-public information through individual reference services while preserving important benefits conferred by this industry.

Despite the laudable efforts of the IRSG Group, important issues related to individual reference services remain. The IRSG principles do not give consumers access to the public information maintained about them and disseminated by the look-up services. Accordingly, consumers will not be able to check for inaccuracies resulting from transcription or other errors occurring in the process of obtaining or compiling the public information by the look-up services. IRSG members have agreed to revisit this issue in eighteen months, and to consider whether to conduct a study quantifying the extent of any such inaccuracies. The Commission strongly urges the IRSG Group to conduct an objective analysis to determine whether the frequency of inaccuracies and the harm associated with them are such that consumer access to public record information or other safeguards are in fact unnecessary.

The Commission also encourages public agencies to consider the potential consequences associated with the increasing accessibility of public records when formulating or reviewing their public records collection and dissemination practices. Furthermore, the Commission is concerned that individuals may be adversely affected by errors in information obtained through look-up services, therefore, the Commission encourages businesses that rely on such information in making adverse decisions (where not already required by law) to voluntarily notify affected consumers of the sources of the information, as long as such notification would not impede law enforcement or fraud prevention. Finally, the Commission acknowledges and encourages the ongoing efforts of many privacy advocates, consumer groups, government agencies, and the IRSG Group to educate the public about information privacy issues. The Commission looks forward to working with all of these groups in this important effort.

Table of Contents

I

Introduction

Computerized database services that sell personal identifying information about consumers -- often referred to as "individual reference services," "look-up services," or "locators" -- drew considerable public and media attention in the fall of 1996. At issue was the perceived sensitivity of the information these computerized database services gather about consumers without their knowledge or consent (*e.g.*, Social Security numbers) and the ease with which such information can be accessed. [1] In October of 1996, three United States Senators reacted to these concerns by requesting that the Federal Trade Commission (the "Commission" or "FTC") conduct a study of these computerized database services (hereinafter "individual reference services," "look-up services," or "services"). [2]

In March of 1997, the Commission announced it would conduct a study of individual reference services used primarily to identify, locate, or verify the identity of an individual. [3] Services used primarily for direct marketing, for obtaining medical and student records, or for purposes subject to the Fair Credit Reporting Act ("FCRA") fall outside the scope of the study. [4] Subsequent to the Commission's announcement, members of the individual reference services industry informed the Commission that they planned to create a self-regulatory framework to address concerns related to their industry. The Commission has since gathered information about the look-up services by soliciting public comments and conducting a public workshop, [5] and Commission staff has engaged in an ongoing dialog with industry members as they worked to craft an effective self-regulatory framework. This report describes (1) the individual reference service industry before implementation of the self-regulatory guidelines, including the types and sources of information available through these services, and how these services are used; (2) the benefits and risks associated with the availability of this information; and (3) the viability of existing and potential controls, including the industry's proposed self-regulatory framework. It concludes with the Commission's recommendations in response to concerns associated with the individual reference services industry

II

The Industry

A. The Overview

Personal identifying information -- information that can be used to identify, locate, or verify the identity of an individual[6] -- has been publicly available for some time. Historically, the government, creditors, insurers, and employers have requested or required from individuals information like name, aliases, address, telephone number, date of birth, and Social Security number; individuals in turn have provided such data in return for certain benefits and services. Moreover, law enforcement agents, private investigators, lawyers, and news reporters have accessed this information for decades in their efforts to track down targets, subjects, heirs, witnesses, etc.

What has happened to make the availability of personal identifying information suddenly spark such far-reaching interest and concern? In recent years, advances in computer technology have made it possible for more detailed identifying information to be aggregated and accessed more easily and cheaply than ever before.[7] In other words, much more richly-detailed data is readily accessible to many more people. Not that long ago, for example, a private investigator hired to track down the location of a non-custodial parent who owed child support would have had to drive around town, from courthouses to county records offices and from the public library to the local department of motor vehicles. Standing in one line to access the records and waiting in another to make copies, he likely would have to fill out forms to send away for still more records from agencies not accessible by car or for records in storage. Ultimately, the investigator would have to sit down and analyze the stacks of paper before him, in the hope of distilling, without the benefit of any information from most out-of-state agencies, his target's current address. This scenario would play out much differently today. Now, by keying in a few search terms at his laptop, in the comfort of his office, an investigator who subscribes to a look-up service can probably track down virtually everything he needs to know to have his target personally served with legal documents. The difference between the costly and time-consuming search once required and the easy and inexpensive retrieval of information now possible can be viewed as a difference in kind, not just degree.[8]

This transformation is due in part to several technological developments. First, data is increasingly available in electronic form.[9] Second, it is now easier to combine data from multiple sources and create comprehensive information products.[10] Third, computer processing speeds have increased.[11] Fourth, the

cost of data storage has dropped dramatically.[12] Finally, personal computers are becoming more affordable,[13] and Internet use is growing more prevalent.[14]

In part due to these developments, the market for personal information, already a multi-billion dollar industry, is growing larger and more diverse.[15] Long-time members of the information industry as well as newcomers are responding to the swelling demand by launching new and increasingly comprehensive personal identifying information products and marketing them to a broadening spectrum of potential customers.[16] As a result, providers of information used to locate, verify, and identify individuals have emerged as a discrete industry.[17]

B. Types and Sources of Information Available

Individual reference service databases contain information about an overwhelming proportion of the population, including children. For example, one prominent individual reference service recently promoted one of its databases as containing the names, current and former addresses, Social Security numbers, and telephone numbers of 160 million individuals.[18] The information is gathered from a wide variety of sources. It typically originates from the consumers themselves, who provide identifying information when they, for example, register to vote, apply for a driver's license, have a new telephone connected, order a catalogue, or apply for credit.[19] Individual reference services then gather this information from public records (like real estate records), publicly available sources (like telephone directories), and from non-public sources (like credit reporting agencies). Alternatively, look-up services may obtain the information from "information vendors," entities that gather data from various sources and either resell it or allow customers to access databases maintained by the information vendors themselves (known as "gateway access").[20] The *types* of information gleaned from these various sources overlap a great deal. For example, an individual's mailing address may be reflected in records obtained from public records, from other public sources, and from non-public sources.

1. Information from Public Records

Public records are a rich source of personal identifying information. Government entities at all levels require individuals to provide various types of information and are usually required to make such records available for public inspection.[21] These records include, but certainly are not limited to, real property records, marriage and divorce records, birth certificates, driving records, driver's licenses, vehicle titles and registrations, civil and criminal court records, parole records, postal service change-of-address records, voter registration records, bankruptcy and lien records, incorporation records, workers' compensation claims, political contributions records, firearms permits, occupational and recreational licenses, filings pursuant to the Uniform Commercial Code (UCC), and filings with the Securities and Exchange Commission (SEC).[22]

Public records may contain extensive and detailed information (*e.g.*, race, gender, Social Security number, address, and dates of birth, marriage, and divorce).[23] Land records, for example, typically include property address and description, dates of sales, sales prices, size of mortgage amounts, and sellers' and purchasers' names.[24] Social Security numbers are available from the records kept by dozens of government entities, such as motor vehicle bureaus and the SEC. Dates of marriage and divorce may be gleaned from

marriage and divorce certificates, respectively. Dates of birth may be available from birth certificates and voter registration records.[25] Professional license records may include name, address, type of license held, and in some cases, the date of the license-holder's last medical examination.[26] Driver's license records[27] make available in one place an individual's name, address, height, weight, gender, eye color, date of birth and, in some cases, Social Security number.[28]

Certain agencies, like the SEC, make records available gratis,[29] but in general government records must be purchased for a nominal fee.[30] For example, the State of New York sells driver's license information in the form of abstracts for approximately five dollars each.[31] These abstracts can include such data as vehicle and ownership information, driver's license records, accident reports, conviction certificates, police reports, complaints, satisfied judgment records, hearing records, and closed suspension revocation orders.[32]

Although government records are increasingly available in electronic form,[33] many still must be transcribed. Individual reference services obtain public records information either directly from the government custodian of records, or indirectly, through information vendors who transcribe it (if necessary) and resell it.[34]

2. Information from Other Public Sources

Publicly available information is another fertile source for personal identifying information. Articles and classified ads in newspapers, magazines, and other publications often provide identifying and background information on individuals.[35] Powerful search engines, now available both through the Internet and proprietary networks, enable people to comb through vast amounts of published materials and find all references to a given individual.[36] White pages directories, whether in paper or electronic form, are a readily accessible source of identifying information. The Internet and CD-ROMs now make it possible to find names, phone numbers, and addresses for people all over the country using one database. Other types of more specialized directories have become prevalent as organizations like alumni groups and professional organizations publish their membership directories on the World Wide Web (the "Web").[37] In fact, many new Web sites may prove to be abundant storehouses of information. Such Web sites include not just personal home pages, where individuals publish their own identifying information as well their hobbies and interests, but also, for example, adoption pages, where separated children and birth parents post their identifying information in the hope of being found.[38]

3. Information from Non-Public Sources

A third general category of information that can be found in these databases is proprietary, or non-public, information, which the individual reference services must purchase. Non-public information includes survey data, data reported by consumers themselves,[39] identifying data contained in "credit headers," as well as marketing and other data.

A "credit header" is the portion of a credit report that typically contains an individual's name, aliases, birth date, Social Security number, current and prior addresses, and telephone number. The three national credit agencies -- Trans Union, Equifax Credit Information Services (hereinafter "Equifax"), and Experian -- maintain and update this information, which they obtain from creditors, courthouses, and the consumers themselves.[40] Trans Union and Experian currently sell credit header information directly to individual reference services or to information vendors who, in turn, sell it to the services.[41] Information in a credit